

SN3262 – Network Administration, Management and Security

Exercise 1: Using Linux Commands to Investigate a Sub-network

Since we will be wanting to look at some simple command line ‘programs’ written in the form of scripts you must be familiar with the material in Exercise 0 and with the various ‘network utilities’ such as *ifconfig*, *netstat*, *ping* and *traceroute*.

1. By reading through the man pages of *ifconfig* what would you say is the function of *ifconfig*?
2. How, previously, have you used *ifconfig*?
3. What would you have to be/have to use this command with the various options?
4. By reading through the man pages of *ping* what would you say is the function of *ping*?
5. If you use broadcast *ping* with the *-c 1* option on a local subnet to which 10 devices, including the broadcasting device, (all set up to respond to broadcast) are attached, how many responses would you get and why?
6. If you use broadcast *ping* with the *-c 2* option on a local subnet to which 10 devices, including the broadcasting device, (all set up to respond to broadcast) are attached, how many responses would you get and why?
7. In the latter case how many of the responses would be marked as duplicates and why?
8. What is the default interval between ‘pings’ and how can it be altered?
9. What would the command *ping 149.170.11.33 -f 0* do and why would you not be able to successfully execute this command?
10. What does the command *ping 149.170.11.33 -l 3* do?
11. What does the command *ping 149.170.11.33 -i 0.1* do and why would you not be able to successfully execute this command?
12. What might the command *ping www.mmu.ac.uk -R* do?

13. If you use broadcast *ping* with the *-w 1* option on a local subnet to which 10 devices, including the broadcasting device, (all set up to respond to broadcast) are attached, how many responses would you get and why?
14. How would the responses to a broadcast *ping* with the *-c 2* option on a local subnet to which 10 devices, including the broadcasting device, (all set up to respond to broadcast) are attached, differ from the responses with the *-w 1* option?
15. By reading through the man pages of *traceroute* what would you say is the function of *traceroute*?
16. *traceroute* normally uses UDP packets. What mechanism is used to “prevent” the receiving host from processing the UDP packet?
17. When *traceroute* is used on a local subnet with the IP address of a host on the subnet which is ‘up’ what information does *traceroute* return?
18. If *traceroute* is used on a local subnet with the IP address of a host on the subnet which is ‘down’ how are the round trip times printed and what does it mean?
19. When *traceroute* is used for a host that is several ‘hops’ away and a router along the path does not send ICMP “time exceeded” messages how is this shown in the output from *traceroute*?
20. Read through the man pages for the *sed* and *gawk* utilities.
You can get more information using the *info* system – e.g. enter *info sed*. Note *q* quits the info system.
Even more help is available from the following web pages:
<http://www.grymoire.com/Unix/Sed.html>
http://www.selectorweb.com/sed_tutorial.html
http://www.cs.utah.edu/dept/old/texinfo/gawk/gawk_toc.html
<http://www.gnu.org/software/gawk/manual/gawk.html>
21. Use *gawk* to print out the first two fields of the line in the */etc/hosts* file that contains the IP address 149.170.13.8. Write down the command line that you used and the output that you obtained.
22. Create a file called *names* as follows:
150.100.100.10: bill
150.100.100.11: fred
150.100.100.12: jim
Use *cat* to list the file and pipe it through *sed* to remove the colons and redirect the output to another file. Check the contents of the file and write down the command line that you used.
23. Read the man pages for *ps*. By piping the output of *ps -ef* to *gawk* determine the number of processes that are running under your user id at the time of running the command — exclude the process for *ps -ef*.